



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/685,656

10/14/2003

W. Todd Daniell

190250-1300

5661

38823

7590

02/04/2009

AT&T Legal Department - TKHR

Attn: Patent Docketing

One AT&T Way

Room 2A-207

Bedminster, NJ 07921

EXAMINER

MACILWINEN, JOHN MOORE JAIN

ART UNIT

PAPER NUMBER

2442

MAIL DATE

DELIVERY MODE

02/04/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/685,656

**Applicant(s)**

DANIELL ET AL.

**Examiner**

John M. MacIwinen

**Art Unit**

2442

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 18 November 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1, 6, 11 - 14, 16 - 17, 19 - 39 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 6, 11 - 14, 16 - 17, 19 - 39 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SF/08)  
Paper No(s)/Mail Date 10/14/2008, 11/17/2008
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments filed 11/18/2008 have been fully considered but they are not persuasive.
2. Applicant begins by repeating arguments made against the Shipp reference regarding whether mail with attachments can be spam. The Examiner's stated in the previous Office Action, mailed 8/21/2008, that:

Paragraph 81 of Shipp states:

*If mail contains attachments, do not log (spam mail currently does not contain attachments).* (Emphasis added)

Shipp thus does not teach away from considering that spam email may contain attachments. Shipp notes, through the use of the word "currently", that spam email does not contain attachments, but also anticipates that spam emails not containing attachments may change in the future. Milliken, the reference cited to teach processing email attachments in relation to spam email, was filed more than a full year after Shipp. Milliken clearly views the situation regarding spam emails containing attachments to have changed. Shipp, by specifically limiting their assertion that spam emails do not contain attachments to the current state in 2002, clearly does not teach away from a future consideration of spam email containing attachments at some other point in time.

Applicant responds by arguing that "Use of the word "currently" does not remedy this fact [that Shipp teaches that spam email does not contain attachments]". Applicant's argument, lacking additional support or citations, is not persuasive.

3. Applicant next argues, regarding claim 1, that the cited art does not teach "sorting the generated tokens in accordance with the corresponding determined spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens."

Woitaszek was cited to teach "where the tokens are sorted in accordance with

the corresponding determined spam probability value", with Tables 4 and 5 cited as support. Applicant argues that "Woitzszek simply includes a table that lists "words indicating nonspam messages" and a table that lists "words indicating spam messages". Applicant continues arguing that "There is no indication that these words are used for any purpose...".

However, Woitaszek clearly describes the purpose. For example, in pg. 1, col. 2, paragraph 2, Woitaszek states

**"The purpose of this project is to** use a SVM to construct an automated classification system to **detect unsolicited email"** (emphasis added).

Woitaszek continues on pg. 1, col. 2, last line, to state that

"The training process produces a weight vector  $w$  with elements corresponding to those in the feature vector  $x$ . In this application, **positive weights indicate that the particular feature is associated with a spam message . . . Any email may be classified as spam** or nonspam by performing a simple dot product between the message's feature vector and the SVM model weight vector . . . **larger values representing stronger characteristics of the classification."**

The "purpose" of Woitaszek thus is clearly to, as Woitaszek states in above excerpt "to detect unsolicited mail"; the "weights" shown in Table 5, as Woitaszek states in above excerpt, are used to derive a spam classification score. Applicant's argument thus is not persuasive.

Applicant continues to argue that "a predefined number of interesting tokens" is not taught. Sahami was relied upon to teach this feature. Applicant never addresses this

reference nor does Applicant addresses the sections cited to teach this feature.

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

4. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. Applicant's arguments continue, however, said arguments repeat the above logic. Said arguments remain unpersuasive for the reasons given above.

#### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shipp (US 2004/0093384 A1) in view of Devine et al. (US 6,968,571 B2), hereafter Devine, further in view of Milliken et al. (US 2004/0073617 A1), hereafter Milliken, further in view of Anderson et al. (US 2004/0064537 A1), hereafter Anderson, further in

view of Uuencode and MIME FAQ

(<http://web.archive.org/web/20021217052047/http://users.rcn.com/wusser/attach.html>), further in view of Gordon et al. (US 6,732,157 B1), hereafter Gordon, further in view of Sahami et al. (A Bayesian Approach to Filtering Junk E-Mail), hereafter Sahami, further in view of Woitaszek and Shaaban (Identifying Junk Electronic Mail in Microsoft Outlook with a Support Vector Machine), hereafter Woitaszek.

8. Regarding claim 1, Shipp shows a method comprising  
receiving an email message from a simple mail transfer protocol (SMTP) server,  
the email message comprising ([0018,0023])

a text body ([0064,0065])

an SMTP email address ([0018,0023,0039,0045,0046])

a domain name corresponding to the SMTP email address ([0039,0045,0046])

an attachment ([0081])

tokenizing the text body to generate tokens representative of words in the text  
([0064-0067])

tokenizing the SMTP email address to generate a token representative of the  
SMTP email address ([0039,0043,0069])

tokenizing the domain name to generate a token that is representative domain  
name ([0022])

as well as showing MD5 hashing ([0093]).

Shipp does not show a 32-bit string indicative of the length of the email message,  
nor does Shipp show tokenizing the attachment and the steps comprising tokenizing

said attachment, determining a probability value for each generated token, selecting a predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability value; performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and categorizing the email message as a function of the generated spam probability.

Devine shows utilizing a 32-bit string in a message header which is indicative of the total length of said message (col. 24 lines 52-67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp with that of Devine in order to better identify message contents so as to facilitate leveraging common code for processing messages (Devine col. 23 lines 60-61).

Shipp in view of Devine do not show tokenizing the attachment.

Milliken shows tokenizing the attachment to generate a token that is representative of the attachment, the tokenizing steps comprising the steps of generating a MD5 hash of the attachment ([0010-0013 and 0052]where MD5 hashes are inherently 128-bit).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine with that of Milliken in order to better identify spam email, as at the time of Shipp's disclosure, spam email was thought "currently" not to be associated with attachments ([81]), an area for which Milliken's more recent disclosure provides updated guidance.

Shipp in view of Devine and Milliken do not show appending the 32-bit string to the generated MD5 hash to produce a 160-bit number.

Anderson shows ([0057-0059]) appending an MD5 hash (inherently 128-bits) to network transmission size information (shown by Devine to be said 32-bit string, and where  $32 + 128$  is inherently 160).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine and Milliken with that of Anderson in order to better uniquely identify messages (Anderson [0057-0059]), leading to improved message spam identification.

Shipp in view of Devine, Milliken and Anderson do not show UUencoding said 160-bit number to generate a token representative of the attachment.

Uuencode and MIME FAQ shows UUencoding a file.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken and Anderson with that of Uuencode and MIME FAQ in order to store the message identification information (represented by the 160-bit number shown by Shipp in view of Devine, Milliken and Anderson) in a format easily exchanged over email (UUencode and MIME FAQ) since UUencoding produces an easily emailed file and since the disclosure of Shipp in view of Devine, Milliken and Anderson relates to email and files transferred over email. Furthermore, UUencoding is a prior art element, as shown in UUencode and MIME FAQ, and thus UUencoding the 160-bit number is combining a prior art element (UUencoding) to known methods (the known methods shown by Shipp in view of

Devine, Milliken and Anderson) to yield predictable results (the results being a UUencoded item).

Shipp in view of Devine, Milliken, Anderson and UUencode and MIME FAQ do not show determining a probability value for each of the generated tokens.

Gordon shows determining a probability value for each of the generated tokens (col. 11 lines 15 –55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson and Uuencode and MIME FAQ with that of Gordon in order to better identify spam elements in messages (Gordon col. 11 lines 15 –55).

Shipp in view of Devine, Milliken, Anderson, UUencode and MIME FAQ and Gordon do not show sorting the generated tokens in accordance with the corresponding determined spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, selecting the predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability value; performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and categorizing the email message as a function of the generated spam probability.

Sahami shows selecting a predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability value to determine a predefined number of interesting tokens, the predefined

number of interesting tokens being a subset of the generated tokens (pg. 4, col. 1, showing having initially “several thousand” features, then selecting 500 of said features after first sorting out features that occur fewer than 3 times (pg. 4, col. 2) and then selecting, of the remaining feature, the 500 features with the highest non-neutral probability value (pg. 6, col. 1, paragraph 1)); performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and categorizing the email message as a function of the generated spam probability (pg. 2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson, Uuencode and MIME FAQ and Gordon with that of Sahami in order to more accurately identify spam email.

Shipp in view of Devine, Milliken, Anderson, UUencode and MIME FAQ and Gordon and Sahami thus do show selecting a subset of the generated tokens based on probability value as well as where the interesting tokens are a subset of the generated tokens (Sahami, pg. 6, col. 1, paragraph 1), but do not show explicitly show where the tokens are sorted in accordance with the corresponding determined spam probability value.

Woitaszek shows where the tokens are sorted in accordance with the corresponding determined spam probability value (Tables 4 and 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson,

Uencode and MIME FAQ, Gordon and Sahami with that of Woitaszek in order to arrange the calculated values in a logical manner, enabling a simple method of extracting the most interesting results (Sahami's disclosure involving selecting said most interesting tokens) via simply taking the top occurring results in Woitaszek's sorted list, as well as to include the abilities to integrate the spam software into a commonly used email program (Woitaszek, Abstract, pg. 1 col. 2).

Shipp in view of Devine, Milliken, Anderson, Uencode and MIME FAQ, Gordon, Sahami and Woitaszek thus show claim 1.

9. Regarding claim 39, Shipp in view of Devine, Milliken, Anderson, Uencode and MIME FAQ, Gordon, Sahami, further in view of Woitaszek show wherein the email is received at a computing device (Milliken, Abstract, Shipp, Abstract).

10. Claims 6, 11, 12, 13, 14, 16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shipp in view of Milliken, Sahami and Woitaszek.

11. Regarding claim, 6 Shipp shows a method comprising receiving an email message comprising a text body ([0064,0065]), an SMTP email address ([0039.0043,0069]), and a domain name corresponding to the SMTP email address ([0039,0045,0046]);

tokenizing the SMTP email address to generate a token representative of the SMTP email address ([0039,0043,0063])

tokenizing the domain name to generate a token representative of the domain name ([0022]), and determining a spam probability value from the generated tokens

((0014,0076)).

Shipp does not show tokenizing the attachment to generate a token that is representative of the attachment.

Milliken shows tokenizing the attachment to generate a token that is representative of the attachment ([10-13 and 51 – 53]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp with that of Milliken in order to better identify spam email, as at the time of Shipp's disclosure, spam email was thought "currently" not to be associated with attachments ([81]); spam and attachments are however an area for which Milliken's more recent disclosure provides updated guidance.

Shipp in view of Milliken, Anderson do not show explicitly show where the tokens are sorted in accordance with the corresponding determined spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens.

Sahami shows selecting a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (pg. 4, col. 1, showing having initially "several thousand" features, then selecting 500 of said features after first sorting out features that occur fewer than 3 times (pg. 4, col. 2) and then selecting, of the remaining feature, the 500 features with the highest non-neutral probability value (pg. 6, col. 1, paragraph 1)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson,

Uuencode and MIME FAQ and Gordon with that of Sahami in order to more accurately identify spam email (Sahami, Abstract).

Shipp in view Milliken and Sahami thus do show selecting a subset of the generated tokens based on probability value as well as where the interesting tokens are a subset of the generated tokens (Sahami, pg. 6, col. 1, paragraph 1), but do not show explicitly show where the tokens are sorted in accordance with the corresponding determined spam probability value.

Woitaszek shows where the tokens are sorted in accordance with the corresponding determined spam probability value (Tables 4 and 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Devine, Milliken, Anderson, Uuencode and MIME FAQ, Gordon and Sahami with that of Woitaszek in order to arrange the calculated values in a logical manner, enabling a simple method of extracting the most interesting results (as discussed by Sahami) via simply taking the top occurring results in Woitaszek's sorted list, as well as to include the abilities to integrate the spam software into a commonly used email program (Woitaszek, Abstract, pg. 1 col. 2).

12. Regarding claim 16, Shipp in view of Milliken, Sahami and Woitaszek further show receiving an email message including a text body (Shipp [0064,0065]).

13. Regarding claim 17, Shipp in view of Milliken, Sahami and Woitaszek further show tokenizing the words in the text body to generate tokens representative of the words in the text body (Shipp [0064,0065]).

14. Regarding claim 23, Shipp in view of Milliken and Woitaszek further show a system comprising a text body (Shipp, [0064,0065]), an SMTP email address (Shipp, [0039.0043,0069]), and a domain name corresponding to the SMTP email address (Shipp, [0039,0045,0046]) and an attachment (Milliken [10-13]);

tokenizing the SMTP email address to generate a token representative of the SMTP email address (Shipp, [0039,0043,0063])

tokenizing logic configured to tokenize the attachment to generate a token that is representative of the attachment (Milliken [10-13 and 51 – 53])

tokenizing the domain name to generate a token representative of the domain name (Shipp, [0022]), and

determining a spam probability value from the generated tokens (Shipp, [0014,0076]) and

sorting logic configured to sort the generated tokens in accordance with the corresponding determined spam probability value (Woitaszek, Abstract, Tables 4 and 5) to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (Sahami, pgs. 4 and 6).

15. Regarding claim 24, Shipp in view of Milliken, Sahami and Woitaszek further show means for receiving an SMTP email address, and a domain name corresponding to the SMTP email address (Shipp, [0039,0045,0046]) and an attachment (Milliken [10-13]);

means for tokenizing the SMTP email address to generate a token representative of the SMTP email address (Shipp, [0039,0043,0063])

means for tokenizing logic configured to tokenize the attachment to generate a token that is representative of the attachment (Milliken [10-13 and 51 – 53])

means for tokenizing the domain name to generate a token representative of the domain name (Shipp, [0022]), and

means for determining a spam probability value from the generated tokens (Shipp, [0014,0076]) and

sorting logic configured to sort the generated tokens in accordance with the corresponding determined spam probability value (Woitaszek, Abstract, Tables 4 and 5) to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (Sahami, pgs. 4 and 6).

**16.** Regarding claim 25, Shipp in view of Milliken, Sahami and Woitaszek further show a computer-readable medium that includes a program, that when executed by a computer, performs the actions of receiving an email message comprising an SMTP email address, ([0039.0043,0069]), a domain name corresponding to the SMTP email address ([0039,0045,0046]) and an attachment (Milliken [10-13]);

tokenizing the SMTP email address to generate a token representative of the SMTP email address ([0039,0043,0063])

tokenizing the attachment to generate a token that is representative of the attachment (Milliken [10-13 and 51 – 53])

tokenizing the domain name to generate a token representative of the domain name ([0022]), and

determining a spam probability value from the generated tokens ([0014,0076])

and

sorting logic configured to sort the generated tokens in accordance with the corresponding determined spam probability value (Woitaszek, Abstract, Tables 4 and 5) to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (Sahami, pgs. 4 and 6).

17. Regarding claim 30, Shipp in view of Milliken, Sahami and Woitaszek further show a system comprising a memory component that stores email logic configured to receive an email message comprising an attachment (Shipp [0018,0023] and Milliken [10-13])),

tokenize logic configured to tokenize the entire attachment to generate a token representative of the attachment (Milliken [10-13 and 70]); and

analysis logic configured to determine a spam probability values from the generated tokens (Milliken [10-13] and Shipp [14,76]) and

sorting logic configured to sort the generated tokens in accordance with the corresponding determined spam probability value (Woitaszek, Abstract, Tables 4 and 5) to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (Sahami, pgs. 4 and 6).

18. Regarding claim 31, Shipp in view of Milliken and Woitaszek further show means for receiving an email message comprising an attachment (Shipp [0018,0023] and Milliken [10-13])),

means for tokenizing the attachment to generate a token representative of the attachment (Milliken [10-13 and 70]); and

means for determining a spam probability values from the generated tokens (Milliken [10-13] and Shipp [14,76])

sorting logic configured to sort the generated tokens in accordance with the corresponding determined spam probability value (Woitaszek, Abstract, Tables 4 and 5) to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (Sahami, pgs. 4 and 6).

19. Regarding claim 32, Shipp in view of Milliken, Sahami and Woitaszek further shows a computer-readable medium that when executed by a computer, performs at least the following: receive an email message comprising an attachment (Shipp [0018,0023] and Milliken [10-13])),

tokenize logic configured to tokenize the entire attachment to generate a token representative of the attachment (Milliken [10-13 and 70]); and determine a spam probability values from the generated tokens (Milliken [10-13] and Shipp [14,76]) and

sort the generated tokens in accordance with the corresponding determined spam probability value (Woitaszek, Abstract, Tables 4 and 5) to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens (Sahami, pgs. 4 and 6).

20. Regarding claims 11 and 26, Shipp in view of Milliken, Sahami and Woitaszek show assigning a spam probability value to the token representative of the SMTP email address (Shipp [0018,0023,0039,0040-0043], Woitaszek, Tables 4 and 5) and

assigning a spam probability value to the token representative of the domain name (Shipp [0022]).

and generating a Bayesian probability values using the spam probability values assigned to the tokens (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

21. Regarding claims 12 and 27 Shipp in view of Milliken, Sahami and Woitaszek further show comparing the generated Bayesian probability value with a predefined threshold value (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

22. Regarding claims 13 and 28 Shipp in view of Milliken, Sahami and Woitaszek further show categorizing the email message as spam in response to the Bayesian probability value being greater than the predefined threshold (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

23. Regarding claims 14 and 29 Shipp in view of Sahami and Milliken further show categorizing the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold (Sahami pg. 6 col. 1).

24. Regarding claims 19 and 35, Shipp in view of Milliken, Sahami and Woitaszek show claim 17 and 34, as well as assigning a spam probability value to each of the tokens representation of the words in the text body (Woitaszek, Tables 4 and 5)

assigning a spam probability value to token representative of the attachment (Woitaszek, Tables 4 and 5, and Milliken, [10-13]),

and generating a Bayesian probability value using the spam probability values assigned to the token (Sahami, pg. 4 col. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Shipp in view of Milliken and Woitaszek with that of Sahami in order to more accurately identify spam email.

25. Regarding claims 20 and 36, Shipp in view of Milliken and Sahami and Woitaszek further show comparing the generated Bayesian probability value with a predefined threshold value (Sahami, pg. 4 col. 2).

26. Regarding claims 21 and 37, Shipp in view of Milliken, Sahami and Woitaszek Sahami further show categorizing the email message as spam in response to the Bayesian probability value being greater than the predefined threshold (Sahami, pg.2, col. 2; pg. 4, col. 2; pg. 6, col. 1).

27. Regarding claims 22 and 38, Shipp in view of Milliken, Sahami and Woitaszek further show categorizing the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold (Sahami, pg. 6 col. 1).

28. Regarding claim 33, Shipp in view of Milliken, Sahami and Woitaszek further show receiving an email message including a text body (Shipp [0064,0065]).

29. Regarding claim 34, Shipp in view of Milliken, Sahami and Woitaszek further show tokenizing the words in the text body to generate tokens representative of the words in the text body (Shipp [0064,0065]).

### ***Conclusion***

30. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew Caldwell/  
Supervisory Patent Examiner, Art  
Unit 2442

John MacIlwain  
(571) 272 - 8686